

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/757,742	01/09/2001	Antony Peng Chew Ng	20879-1.00US	7729

20350 7590 08/09/2004

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER

NGUYEN, MINH DIEU T

ART UNIT
2137

DATE MAILED: 08/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/757,742	NG ET AL.
	Examiner	Art Unit
	Minh Dieu Nguyen	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 01/09/2001.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-5 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-5 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ .

5) Notice of Informal Patent Application (PTO-152)

6) Other: ____ .

DETAILED ACTION

1. Claims 1-5 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-5 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As to claim 1, line 11 page 8, the phrase "said interval key"; line 16 page 8, the phrase "the common interval key"; "said common interval index"; line 18 page 8, the phrase "said system" and line 19 page 8, the phrase "said common interval key" lack antecedent basis.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. **Claims 1-5** are rejected under 35 U.S.C. 103(a) as being unpatentable

over Bao et al., WO 00/57595 in view of Young et al., US 6,473,508.

a) **As to claim 1**, Bao discloses a method and apparatus for encrypting and decrypting digital data for the purpose of protecting or securing its contents comprising the steps of dividing the data into data segments (Fig. 1 element 100), each bit is associated with a different clock cycle and thus segment and interval are both equivalent to time interval; extracting at each party a common benchmark; agreeing among each party on a starting interval key referenced to the common benchmark (lines 11-13, page 3), Bao discloses the step of accepting at least a key shared with the decrypting party, thus a handshake or agreement has taken place; causing each party to generate iteratively a next interval key independently of each other party but with reference to an interval index, wherein the interval index is encrypted by the public key (lines 6-12, page 6), the segment key reads on the interval key, Bao further discloses segment keys are generated not only on the cryptographic key k, but also on previous segment keys (lines 27-32, page 8), thus previous segment is encrypted by a key, in this case public key could be used; initiating a secure communication between parties using reference to the interval index, not their respective interval keys (lines 5-7, page 7); causing each party to encrypt a message to be secured using the common interval key independently computed based on the common interval index (lines 14-22, page 3) and causing the encrypted message to be communicated such that the encrypted message can

be decrypted using the common interval key (lines 30-33, page 3 to lines 1-8, page 4).

Bao does not disclose an escrow agent generating public and private keys to all parties within a communication system.

Young discloses a key distribution center, which reads on an escrow agent, communicates public key to users (col. 1, lines 25-35).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ a key distribution center as an escrow agent or certification authority who is trusted by all parties to give correct keys information, as Young teaches, in the system of Bao so as to strengthen the security of communication channels.

b) **As to claim 2**, Bao discloses the parties exchange their respective interval indexes and wherein the parties with the older interval indexes advance their interval index and compute the interval key corresponding to the latest interval index (lines 12-27, page 3). Bao discloses the parties share a secret key, initial value and other functions, thus it is a mutual agreement to exchange the data segment index ($I=1, 2, \dots$), which reads on interval index, not interval key.

c) **As to claim 3**, the examiner takes official notice that use of destroying old key after a new key is generated is quite well known in the data encryption art.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of destroying old key once the new key is generated in the system of Bao and Young so as to make the system even more secure.

d) **As to claims 4 and 5**, the interval index and starting interval key are not communicated to the escrow agent. These information are only exchanged between parties involved in communication channels (lines 28-31, page 5).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure

a) US 6,731,758 to Graunke et al. discloses digital video content transmission ciphering and deciphering method and apparatus.

b) US 6,330,671 to Aziz discloses method and system for secure distribution of cryptographic keys on multicast networks.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 703-305-9727. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 703-306-3036. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Minh Dieu Nguyen
Examiner
Art Unit 2137

MDN
7/19/04

Andrew Caldwell
Andrew Caldwell